Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2018 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2018

Phishing Susceptibility across Industries: The Differential Impact of Influence Techniques

Chuan Tian
University of Oklahoma Norman Campus

Matthew L. Jensen
University of Oklahoma Norman Campus

Alexandra Durcikova
University of Oklahoma Norman Campus

Phishing Susceptibility across Industries: The Differential Impact of Influence Techniques

Chuan (Annie) Tian[1]
MIS Division, University of Oklahoma
Norman, OK, USA

Matthew L. Jensen
MIS Division, University of Oklahoma
Norman, OK, USA

Alexandra Durcikova
MIS Division, University of Oklahoma
Norman, OK, USA

ABSTRACT

Organizations are increasingly becoming the target of phishing attacks, and victimization is typically accompanied by financial loss, disclosure of private information, and reputational damage. Building on existing persuasion and phishing literature, we argue that shared industry practices, values, and assumptions alter the effectiveness of phishing influence techniques. We tested our hypotheses with a quasi-experiment (n = 10,967) using a secondary dataset containing the results of mock phishing attacks sent to 30 finance and 15 non-finance organizations. Results demonstrated variability in susceptibility to phishing influence techniques due to industry. Consistent with our theorizing, phishing techniques such as liking were more effective among non-finance organizations and social proof, reciprocity, and authority were more effective among finance organizations. These findings address past inconsistencies in empirical phishing research and offer support for a more nuanced perspective concerning phishing susceptibility due to industry characteristics. Theoretical and practical implications are discussed.

Keywords: Phishing, Deception, Self-Determination Theory, Persuasion, Influence Techniques, Finance, Organizational Characteristics, Organizational Culture

[1] Corresponding author. Chuan.Tian-1@ou.edu +1 (405) 325-0770

INTRODUCTION

In today's interconnected world, social engineers are applying their skills to the cyber realm to take advantage of others. Among the most evident applications of social engineering is phishing, in which attackers imitate messages from legitimate sources and try to extract valuable information (e.g., credentials, private information) from their recipients. Examples of recent successful phishing attacks litter the news. In January 2017, reports emerged alleging phishing as the cause behind the release of private campaign emails during the United States presidential contest (CBS News 2016). In May 2017, Google confirmed that approximately one million Gmail accounts were compromised by sophisticated phishing attacks which appeared as Google Docs but spread malware that let phishers gather email history, access e-business portals (e.g., Amazon), and reach online banking sites (NBCNews 2017). Phishing is one of the most common ways people are exploited on the internet (Muscanell et al. 2014) and despite media attention and highly publicized attacks, individuals still succumb.

Since the scourge of phishing has been increasing in frequency and sophistication, researchers have attempted to gain a greater understanding regarding phishing susceptibility and have called for more investigation of this organizational threat (e.g., Wright and Marett 2010). Understanding the factors that contribute to phishing susceptibility can lead to more effective training interventions and technical protections. For example, a prominent contributor to phishing susceptibility is the influence technique that is employed during the phishing attack. Wright et al. (2014) discovered that some influence techniques (e.g., liking and social proof) were more effective in generating compliance with phishing messages than other influence techniques (e.g., authority). They argued that awareness of effective phishing techniques built resistance among potential recipients as individuals become able to recognize the techniques as they are used against them. However, other researchers (Butavicius et al. 2016) uncovered divergent results suggesting that

authority is most effective in generating compliance. These inconsistent results suggest that additional factors are likely at work in explaining the relationship between influence techniques and susceptibility to phishing attacks.

To reconcile inconsistent findings from prior research and achieve a more complete understanding of phishing susceptibility, we expand the investigation of influence techniques used in phishing messages and examine how industry context enables or suppresses the effectiveness of phishing influence techniques. We draw on the Self-Determination Theory (SDT) (Deci and Ryan 1985), which addresses primary motivations for why individuals comply with persuasive requests, to explain the variability in phishing susceptibility. We conducted a quasi-experiment using a dataset collected by a professional information technology (IT) services company (CompA[2]). CompA conducted mock phishing attacks against 10,967 individuals in 45 companies using a series of proprietary mock phishing messages. We manually coded the content to determine which influence techniques were employed in each message. We then examined differences in susceptibility to phishing influence techniques between industries.

THEORETICAL BACKGROUND

Succumbing to phishing messages has often been examined through the lens of persuasion since attackers are attempting to get their targets to comply with requests (e.g., click on a link, open an attachment) (Goel et al. 2017). Scholars exploring persuasion (Cialdini 2009) have identified six prototypical techniques that individuals use to influence others: liking, reciprocity, social proof, consistency, authority, and scarcity. These influence techniques have been observed in a variety of settings and have successfully produced compliance in diverse contexts such as marketing (Cialdini and Rhoads 2001) to public health campaigns (Dunlop et al. 2010), and more nefarious areas like social engineering (Mitnick and Simon 2001).

[2] The identity of the company is hidden to protect privacy.

According to phishing researchers (Wright et al. 2014), each technique has been tied to a motivational base in SDT (Deci and Ryan 1985) including intrinsic, identification, introjected, and external motivations. Liking has been associated with intrinsic motivation, which is based on enjoyment, similarity, and affiliation. Social proof and scarcity have been associated with identification motivation and concern the attainment of one's goals (e.g., acquiring of resources). Reciprocity and consistency have been associated with introjected motivation, which is based on societal pressures and living up to community expectations. Finally, authority has been associated with external motivation and legitimate power to reward or punish.

Phishing Influence Techniques and Susceptibility

Scholars have begun exploring the relative effectiveness of influence techniques to further understand which techniques are most successful and which are easiest to identify. For example, in coding actual phishing message to determine the prevalence of influence techniques, Ferreira et al (2015) found that liking was the most prevalent and argued that this technique was effective because it relates most to how people interact with each other. Wright et al (2014) used a mock phishing field experiment involving university students to discover differences in effectiveness among the influence techniques. They found that liking, scarcity, and social proof techniques, which respectively appeal to intrinsic and identification motivations, generated the most responses to phishing attacks. These techniques grant self-determination to receivers and leave them free to choose to comply. Authority, which appeals to external motivation and reduces self-determination, was least effective in generating responses. However, other researchers found that authority was most effective in persuading individuals to comply with phishing messages. In a laboratory study using undergraduate students, Butavicius et al. (2016) found that messages invoking authority were seen at the safest to click. In a large field experiment involving 62,000 public sector employees who regularly interface with the public and handle highly sensitive data, Williams et al (2018) found that persuasion attempts

using authority techniques increased the likelihood that individuals would click on malicious links. The inconsistency of the results across several lab and field studies suggest that other factors may moderate the effect of influence techniques on phishing susceptibility.

Past research on motivation and compliance has shown that alignment between the message and the receivers' expectations and context is especially important to achieve (Deci and Ryan 1985). Further, Cialdini and others (Martin et al. 2014) acknowledged the importance of the environment in which influence techniques are used and suggested that in addition to message contents in human interaction, contextual factors can also dramatically enhance or diminish likelihood of compliance. The notion of alignment between message and context is particularly salient in phishing attacks because the phishers' objective is to mimic legitimate messages from credible sources (Wright and Marett 2010). If messages attempt to induce action by appealing to motivational bases (e.g., intrinsic, external), the attempts will be much more likely to succeed if the recipients are receptive to the motivational appeal and the appeal is relevant to them in the context in which the message is received. But, relevant motivations for taking action may change depending on industry context.

Phishing Influence Techniques and Industry Characteristics

In considering how industry characteristics might alter the effect of phishing influence techniques, we focused on resolving the contradictory findings of phishing susceptibility in response to influence techniques appealing to intrinsic and external motivational bases. We attempted to identify an industry whose members may respond to these techniques differently and settled on the finance industry, which includes service providers in banking, credit unions, investing, lending, insurance, securities trading, and securities issuance. The finance industry represents a significant part of the US economy and is a frequent target of phishers who are chasing lucrative access to accounts or valuable data to resell.

Some have argued that organizations in the financial industry are evolutionarily adaptive (Tett 2009) and display characteristics such as hyper competition and hyper motivation (Langevoort 2011). Financial organizations incentivize instrumental rationality in pursuit of private gain, as costs for small deviations can be high (e.g., Hilton 2003). Common industry practices such as selection and hiring, socialization, and reward structures for performance (e.g., bonuses) may reinforce evolutionary adaptiveness and instrumental rationality. Further, on average, individuals in the financial industry display elevated levels of narcissism and self-enhancement compared to individuals in other industries (Furnham et al. 2014). Elevated narcissism is associated with heightened levels of self-efficacy and risk acceptance (Sedikides et al. 2004) and lower levels of interpersonal warmth and sympathy (Campbell et al. 2007). Therefore, we expect that industries fostering instrumental rationality and self-enhancement will likely affect which phishing influence techniques are most persuasive.

HYPOTHESIS DEVELOPMENT

The success of the liking influence technique depends on individuals' tendency to say yes to people that they "know and like" (Cialdini 2009, p. 142). It is based on intrinsic motivation and uses a sense of familiarity and preference. It can be deployed by referencing common interests and emphasizing similarity between a message sender and receiver (Ryan et al. 1985). Individuals respond to an influence attempt using liking because they think they want to and there is often little tangible payoff for compliance. The absence of a tangible payoff is incongruent with elevated narcissism and accompanying lower levels of interpersonal warmth and sympathy for others for individuals in the finance industry. If recipients are to expend time and attentional resources processing messages at work, those in finance industry are likely to expect some kind of reward or return. Without the promise of a tangible payoff, we expect industry pressures of instrumental rationality to undermine the liking influence technique. Additionally, intense competition and

incentive mechanisms in the finance industry may foster an environment in which individuals are less receptive to emotional appeals (Gigerenzer and Todd 1999).

> *H1: The relationship between the liking influence technique and phishing susceptibility will be lower in the finance industry than in non-finance industries.*

Contrary to liking, other influence techniques are more closely associated with an explicit or implied payoff. The promise of a tangible payoff aligns to a greater degree with practices, values, and assumptions within the finance industry. Therefore, these techniques, when employed in the message body, may be more effective in inducing individuals in finance organizations to comply with phishing requests.

First among these techniques is social proof, which similarly to liking, also affords a high degree of self-determination. However, rather than intrinsic motivation, social proof appeals to identification motivation, which emphasizes individual goal attainment and advancement (Deci and Ryan 1985). When people are unsure of how to behave, they will often look to others for cues concerning appropriate behavior (Aronson et al. 2005). In phishing messages, social proof is often invoked using statements or cues claiming many others have benefitted from performing the requested action and the targeted individuals should too. Individuals responding to social proof influence techniques are motivated to comply because of an explicit payoff that has been claimed by others. Pursuit of payoffs aligns with instrumental rationality and pursuit of private gain.

> *H2: The relationship between the social proof influence technique and phishing susceptibility will be higher in the finance industry than in non-finance industries.*

The reciprocity influence technique is activated when the phisher creates the impression that he or she has done something to benefit the targeted individual (e.g., notifying them about some opportunity or problem) and the phisher asks the individual to perform some action in return (e.g., clicking on a link, downloading malware). The reciprocity influence technique is tied to introjected motivation (Deci and Ryan 1985), which is based on self-image pressures such as living up to

expectations. We argue that individuals in the finance industry may be more susceptible to reciprocity for two reasons. First, reciprocity taps into a transactional perspective where information or a service is ostensibly provided in exchange for something in return. The transactional nature of reciprocity will likely be better understood and accepted by individuals operating under instrumental rationality. Second, the prevalence of self-enhancement within the finance industry may lead individuals to be highly concerned with their image and reputation. Consequently, they may be more likely to respond to influence techniques that leverage image pressures.

H3: The relationship between the reciprocity influence technique and phishing susceptibility will be higher in the finance industry than in non-finance industries.

Authority influence technique, which is based on external motivation, may directly feed self-enhancement and the pursuit of private gain. In phishing attacks, authority is most often used when phishers impersonate someone with legitimate authority and threaten negative consequences for non-compliance or promise rewards for compliance. The explicit tie to a payoff may make the authority more effective for individuals in finance industry. Studies on fiduciary business found that employees are more likely to exhibit loyalty to authority and power under higher institutional pressure (Rick and Loewenstein 2008). Further, instrumental rationality may promote obedience to authority as a more rational response to requests than defiance. Finally, high incentives (e.g. bonuses and awards) in the finance industry may also encourage widespread acceptance of and compliance with authority.

H4: The relationship between the authority influence technique and phishing susceptibility will be higher in the finance industry than in non-finance industries.

METHOD

To hypotheses, our experiment compared the results of mock phishing attacks in the finance industry to mock phishing results in other industries. CompA manages IT security for clients around the world and as part of these services, it performs mock phishing attacks to test client vulnerability

to actual phishing attacks. The results of these mock phishing attacks are then shared with organization leaders for use in understanding the need for training and other interventions. To explore the effectiveness of these mock phishing attacks, we gathered the messages used in the attacks, rated the influence techniques used in each message, and then examined the effectiveness of each message across finance and non-finance industries.

Message Sample

CompA created eight mock phishing messages which were sent to a total of 10,967 employees in 45 different organizations.[3] These organizations belong to eight different industries, including government, manufacturing, education, biotechnology, energy, retail, technology, and finance. Of the 45 client organizations, 30 are in the financial industry. All phishing messages encouraged recipients to click on links embedded in the text of the message. If a recipient clicked on a link, the individual would be directed to a fabricated webpage designed to appear legitimate. The fabricated webpage would solicit from individuals their credentials (e.g., username and password).

Measurement

The first explanatory variable was a binary variable describing whether each organization was a member of the financial industry. To preserve privacy, identities of organizations were kept confidential from the authors. Therefore, membership in the finance industry was determined by CompA. Organizations in the financial industry were assigned a value of 1. Organizations outside of the financial industry (e.g., government, manufacturing, education, biotechnology, energy, retail, and technology) were assigned a value of 0.

Next, the content of the 8 mock phishing messages were rated concerning the influence techniques they invoked. Rating of the influence techniques (liking, social proof, reciprocity, and authority) was performed by four trained raters who received approximately two hours of training

[3] The phishing messages are proprietary and are not able to be shared, but brief descriptions of each message are shared in Table 4.

prior to rating the mock phishing messages. The presence of each influence technique was recorded on a 1-7 scale with 1 indicating absence of the technique and 7 indicating the technique was very much present. A satisfactory level of agreement (e.g., interclass correlations were greater than 0.7) was achieved for all the ratings (Nunnally et al. 1967). For messages where raters' scores did not exactly align, an average of the scores was performed. The average ratings and interclass correlations (ICCs) for each of the influence techniques in message content are shown in Table 1.

Table 1 Average Ratings of Influence Techniques and ICC Statistics

Message Description	Total Non-Finance Messages	Total Finance Messages	Liking	Social Proof	Reciprocity	Authority
Fraud	-	34	2.25	1.00	5.00	3.75
Data Breach	-	189	3.25	1.00	3.00	3.75
Browser Restrictions	418	321	2.50	1.00	1.00	5.00
Electronic Fax	-	435	4.25	1.00	3.00	2.5
Social Media Invitation 1	775	107	5.25	3.00	4.75	2.75
Social Media Invitation 2	836	1669	5.25	4.75	3.5	3.00
Software Update	301	335	2.50	1.00	2.00	5.75
Email Warning	5274	273	4.25	1.00	4.00	6.00
ICC			.94	.98	.96	.98
Total/Mean (SD)	7604	3363	4.32 (.85)	2.02 (1.58)	3.57 (.91)	4.79 (1.45)

To judge the effectiveness of mock phishing messages, we follow the past research on phishing susceptibility and use click-throughs (CTs) as the dependent variable (Goel et al. 2017; Jensen et al. 2017; Wright et al. 2014), because being directed to a malicious site where devices could be compromised is a common attack strategy. CTs are also widely used in marketing research and capture the effectiveness of online advertisement and email campaigns (Richardson et al. 2007). A CT is a binary variable that is coded as 1 if an individual clicks on the link embedded in the message or 0 if an individual does not does not click on the link.

RESULTS

Descriptive CT results for each message sent to individuals in non-finance and finance industries are shown in Table 2. The CT rate was 20% for the finance industry and 8% non-finance industries.

Table 2. Rates of CTs for Non-Finance and Finance Industries

Message	Non-Finance CT Rate (%)	Finance CT Rate (%)	Total (%)
Fraud	-	12 (0.35)	12 (0.35)
Data Breach	-	11 (0.06)	11 (0.06)
Browser Restrictions	61 (0.15)	111 (0.35)	172 (0.23)
Electronic Fax	-	153 (0.35)	153 (0.35)
Social Media Invitation 1	165 (0.21)	11 (0.10)	176 (0.20)
Social Media Invitation 2	184 (0.22)	322 (0.19)	506 (0.20)
Software Update	7 (0.02)	16 (0.05)	23 (0.04)
Email Warning	162 (0.03)	26 (0.10)	188 (0.03)
Total	579 (0.08)	662 (0.20)	1241 (0.11)

To test if the effectiveness of the influence techniques varied by industry, we a performed a logistic regression with membership in the finance industry and ratings of phishing influence techniques as explanatory variables and whether each recipient clicked on the link in the phishing message the response variable. The logistic regression accommodated the binary dependent response variable and the interactions between binary and continuous explanatory variables. The results of the logistic regression are shown in Table 3.

Table 3. Logistic regression results

Variable	B	S.E.	Wald	Sig. (df = 1)
Constant	0.326	0.888	0.135	0.714
Finance	0.717	1.136	0.399	0.528
Liking	1.779	0.646	7.585	0.006
Social Proof	-0.778	0.262	8.849	0.003
Reciprocity	-1.302	0.373	12.187	<0.001
Authority	-0.892	0.075	140.597	<0.001
Finance x Liking	-1.445	0.675	4.586	0.032
Finance x Social Proof	0.621	0.269	5.342	0.021
Finance x Reciprocity	0.665	0.391	2.894	0.089
Finance x Authority	0.473	0.109	18.887	<0.001

Notes. Omnibus test of model coefficients: χ^2 (9, N = 10967) = 987.69, p <.001; -2 Log likelihood: 6756.48; Nagelkerke R^2: .170; Hosmer and Lemeshow test: 0.283

Consistent with our hypotheses, significant interaction effects between industry and influence technique emerged for liking, social proof, and authority. Further, the interaction effect including reciprocity approached significance. These findings support H1, H2, and H4 and marginally support H3.

DISCUSSION

Previous research using persuasion theory (Ferreira et al. 2015; Wright et al. 2014) argued that influence techniques offering higher self-determination (e.g., liking) would be more effective than techniques offering a lower degree of self-determination (e.g., authority). But, other researchers (Williams et al. 2018) examined the same phishing influence techniques and found that authority was most influential. This research corroborates the techniques' variability in phishing effectiveness uncovered by past research and it was noted not only among the phishing messages, but also among the influence techniques that were used *across* messages. Consistent with Wright et al., we discovered that the main effect from liking was positive and among the most prominent of the effects we tested. Additionally, the main effect from authority was negative. However, we also noted the negative main effects from social proof and reciprocity, which were opposite from what has been demonstrated in past research. The inconsistency we observed, when joined by findings from others, suggests that other factors aside from the direct effects of phishing influence techniques contribute to phishing susceptibility.

To account for the possibility of variable effects from phishing message characteristics we adopted a contextualization approach to theory development (Bamberger 2008; Hong et al. 2013). We identified industry as a salient, collective contextual factor influencing how each individual employee reacts to certain influence tactics employed in phishing attacks. Chiasson and Davidson (2005) have argued that industry has received little academic attention in IS research despite its

considerable impact on IS phenomena and that it provides critical "contextual space" to develop new theory and assess the boundaries of existing theories. Our results corroborate these arguments. We found that certain industries (e.g., finance) have characteristics that are sufficiently homogeneous that they can alter susceptibility of their members to phishing influence techniques.

We incorporated theory that explicitly addresses alignment between message and industry characteristics and demonstrated that industry practices, values, and assumptions offer an explanation regarding why certain phishing influence techniques are more effective in some organizations, but not others. We demonstrated that these differences in phishing influence techniques exist across industries. By demonstrating variability in message effects and supporting alignment between message and context, researchers will be better able to accurately represent important nuances driving phishing susceptibility and will be better equipped to counter phishing risks to which organizations in certain industries are uniquely vulnerable. Cognizance of specific vulnerabilities resulting from industry membership provides promising avenues for developing training and other interventions to help organization members become more resistant to such attacks. These interventions may include awareness campaigns, inoculation efforts, and attention allocation training (Jensen et al. 2017; Kumaraguru et al. 2010). Also, prior research has found that simply making individuals aware of how influence techniques may affect them can make individuals more resistant to the techniques (Cialdini 2009).

LIMITATIONS AND FUTURE STEPS

First, the sampling and administration of the treatments in the quasi-experiment were determined by CompA and were not random. However, the large sample size of 10,967 mock phishing emails still supplies us with strong confidence in the generalizability of our findings. The negative main effects for social proof for scarcity suggest that there may be other moderators altering individual susceptibility to phishing influence techniques. We have speculated several possibilities,

but these speculations require additional investigation. Second, there are numerous other organizational characteristics that may influence susceptibility to phishing attacks.

REFERENCES

Aronson, E., Wilson, T. D., and Akert, A. 2005. "Social Psychology. 2005." Upper Saddle River, NJ: Prentice Hall.

Bamberger, P. 2008. "From the Editors Beyond Contextualization: Using Context Theories to Narrow the Micro-Macro Gap in Management Research." Academy of Management Briarcliff Manor, NY.

Butavicius, M., Parsons, K., Pattinson, M., and McCormac, A. 2016. "Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails," *arXiv preprint arXiv:1606.00887*).

Campbell, W. K., Bosson, J. K., Goheen, T. W., Lakey, C. E., and Kernis, M. H. 2007. "Do Narcissists Dislike Themselves "Deep Down Inside"?," *Psychological Science* (18:3), pp. 227-229.

CBS News. 2016. "The Phishing Email That Hacked the Account of John Podesta."

Chiasson, M. W., and Davidson, E. 2005. "Taking Industry Seriously in Information Systems Research," *Mis Quarterly*), pp. 591-605.

Cialdini, R. B. 2009. *Influence: Science and Practice*. Pearson Education Boston, MA.

Cialdini, R. B., and Rhoads, K. V. 2001. "Human Behavior and the Marketplace," *Marketing Research* (13:3), p. 8.

Deci, E. L., and Ryan, R. M. 1985. "The General Causality Orientations Scale: Self-Determination in Personality," *Journal of research in personality* (19:2), pp. 109-134.

Dunlop, S. M., Wakefield, M., and Kashima, Y. 2010. "Pathways to Persuasion: Cognitive and Experiential Responses to Health-Promoting Mass Media Messages," *Communication Research* (37:1), pp. 133-164.

Ferreira, A., Coventry, L., and Lenzini, G. 2015. "Principles of Persuasion in Social Engineering and Their Use in Phishing," *International Conference on Human Aspects of Information Security, Privacy, and Trust HAS 2015,* T. Tryfonas and I. Askoxylakis (eds.): Springer, pp. 36-47.

Furnham, A., Hyde, G., and Trickey, G. 2014. "Do Your Dark Side Traits Fit? Dysfunctional Personalities in Different Work Sectors," *Applied Psychology* (63:4), pp. 589-606.

Gigerenzer, G., and Todd, P. M. 1999. *Simple Heuristics That Make Us Smart*. Oxford University Press, USA.

Goel, S., Williams, K., and Dincelli, E. 2017. "Got Phished? Internet Security and Human Vulnerability," *Journal of the Association for Information Systems* (18:1), p. 22.

Hilton, D. J. 2003. "Psychology and the Financial Markets: Applications to Understanding and Remedying Irrational Decision-Making.," in *The Psychology of Economic Decisions (Vol. 1): Rationality and Well-Being,* I. Brocas and J.D. Carrillo (eds.). Oxford, UK: Oxford University Press.

Hong, W., Chan, F. K., Thong, J. Y., Chasalow, L. C., and Dhillon, G. 2013. "A Framework and Guidelines for Context-Specific Theorizing in Information Systems Research," *Information Systems Research* (25:1), pp. 111-136.

Jensen, M. L., Dinger, M., Wright, R. T., and Thatcher, J. B. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems* (34:2), pp. 597-626.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., and Hong, J. 2010. "Teaching Johnny Not to Fall for Phish," *ACM Transactions on Internet Technology (TOIT)* (10:2), p. 7.

Langevoort, D. C. 2011. "Psychological Perspectives on the Fiduciary Business," *BUL Rev.* (91), p. 995.

Martin, S. J., Goldstein, N., and Cialdini, R. 2014. *The Small Big: Small Changes That Spark Big Influence*. Hachette UK.

Mitnick, K. D., and Simon, W. L. 2001. *The Art of Deception: Controlling the Human Element of Security*. Wiley. com.

Muscanell, N. L., Guadagno, R. E., and Murphy, S. 2014. "Weapons of Influence Misused: A Social Influence Analysis of Why People Fall Prey to Internet Scams," *Social and Personality Psychology Compass* (8:7), pp. 388-396.

NBCNews. 2017. "Massive Phishing Attack Targets Gmail Users," in: *NBC News*

Nunnally, J. C., Bernstein, I. H., and Berge, J. M. t. 1967. *Psychometric Theory*. JSTOR.

Richardson, M., Dominowska, E., and Ragno, R. 2007. "Predicting Clicks: Estimating the Click-through Rate for New Ads," *Proceedings of the 16th international conference on World Wide Web*: ACM, pp. 521-530.

Rick, S., and Loewenstein, G. 2008. "Hypermotivation," *Journal of Marketing Research* (45:6), pp. 645-648.

Ryan, R. M., Connell, J. P., and Deci, E. L. 1985. "A Motivational Analysis of Self-Determination and Self-Regulation in Education," *Research on motivation in education: The classroom milieu* (2), pp. 13-51.

Sedikides, C., Rudich, E. A., Gregg, A. P., Kumashiro, M., and Rusbult, C. 2004. "Are Normal Narcissists Psychologically Healthy?: Self-Esteem Matters," *Journal of personality and social psychology* (87:3), p. 400.

Tett, G. 2009. *Fool's Gold: How the Bold Dream of a Small Tribe at Jp Morgan Was Corrupted by Wall Street Greed and Unleashed a Catastrophe*. Simon and Schuster.

Williams, E. J., Hinds, J., and Joinson, A. N. 2018. "Exploring Susceptibility to Phishing in the Workplace," *International Journal of Human-Computer Studies* (120), pp. 1-13.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., and Marett, K. 2014. "Research Note-Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance," *Information systems research* (25:2), pp. 385-400.

Wright, R. T., and Marett, K. 2010. "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived," *Journal of Management Information Systems* (27:1), pp. 273-303.